The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
05/10/2016

SUBJECT:
Cumulative Security Update for Internet Explorer (MS16-051)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Internet Explorer. These vulnerabilities could allow an attacker to execute code in the context of the browser if a user views a specially crafted web page. An attacker who successfully exploited the vulnerabilities could gain the same user rights as the current user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Microsoft Internet Explorer is prone to multiple vulnerabilities that could allow remote code execution. The vulnerabilities are as follows:

- Multiple memory corruption vulnerabilities exist in the way Jscript and VBScript engines render when handling objects in memory (CVE-2016-0187,CVE-2016-0189)

- A security feature bypass vulnerability exists in the UMCI component of Device Guard when it improperly validates code integrity (CVE-2016-0188)
- A memory corruption vulnerability when Internet Explorer improperly accesses objects in memory (CVE-2016-0192).
- An information disclosure vulnerability exists when Internet Explorer does not properly handle file access permissions (CVE-2016-0194).

The most severe of these vulnerabilities could allow an attacker to execute remote code by luring a victim to visit a specially crafted malicious website. When the website is visited, the attacker's script will run within the context of the affected browser or with the same permissions as the affected user account. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- A workaround for CVE-2016-0187 and CVE-2016-0189 is to restrict access to VBScript.dll. The command line instructions to accomplish this are available in Microsoft Security Bulletin MS16-051.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/library/security/ms16-051.aspx

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0187
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0188
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0189
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0192
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0194